

Department of Mental Health
TRANSMITTAL LETTER

SUBJECT		
DMH Privacy Policies and Procedures		
POLICY NUMBER	DATE	TL#
DMH Policy 645.1	JUL 16 2003	28

Purpose. To implement guidelines and procedures consistent with federal and District law that protect the privacy of our consumers' health information. The governing privacy guidelines are described in this policy. Specific topics and procedures are addressed in the Department of Mental Health (DMH) Privacy Policies and Procedures Operations Manual. The manual shall be disseminated throughout the Department and made available to Network providers.

Applicability. DMH and its participating Network providers.

Network means an organized health care arrangement consisting of DMH, and every mental health provider that is certified, licensed, or otherwise regulated by DMH, or has entered into a contract or agreement with DMH for the provision of mental health services or mental health supports.

This policy replaces any requirements in existing Department policies that may contain different information relating to confidentiality of mental health information. Those policies shall be revised accordingly.

Policy Clearance. Reviewed by affected responsible staff, including DMH General Counsel, DMH, CSA and SEH Privacy Officers and others.

Implementation Plans. A plan of action to implement or adhere to this policy must be developed by designated responsible staff. If materials and/or training are required to implement this policy, these requirements must be part of the action plan. Specific staff should be designated to carry out the implementation and program managers are responsible for following through to ensure compliance. Action plans and completion dates should be sent to the appropriate authority. Contracting Officer Technical Representatives (COTRs) must also ensure that contractors are informed of this policy if it is applicable or pertinent to their scope of work. *Implementation of all DMH policies shall begin as soon as possible. Full implementation of this policy shall be completed within sixty (60) days after the date of this policy.*

Policy Dissemination and Filing Instructions. Managers/supervisors of DMH and DMH contractors must ensure that staff are informed of this policy. Each staff person who maintains policy manuals must promptly file this policy in Volume I of the blue **DMH** Policy and Procedures Manual, and contractors must ensure that this policy is maintained in accordance with their internal procedures. *A copy of this policy must also remain in the Privacy Policies and Procedures Operations Manual, which must be located in all programs that use and disclose PHI (See Section 13 of the policy).*

(See Back)

*If any CMHS or DMH policies are referenced in this policy, copies may be obtained from the DMH Policy Support Division by calling (202) 673-7757.

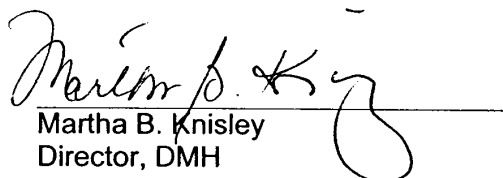
ACTION


REMOVE AND DESTROY

**CMHS 50000.645.1
(dated September 8, 1988)**

INSERT

**DMH Policy 645.1, and
see filing instructions above.**


Martha B. Knisley
Director, DMH

GOVERNMENT OF THE DISTRICT OF COLUMBIA  DEPARTMENT OF MENTAL HEALTH	Policy No. 645.1	Date JUL 16 2003	Page 1
	Supersedes CMHS 50000.645.1, Confidentiality of Records Guidelines, dated September 8, 1988		
Subject: DMH Privacy Policies and Procedures			

1. **Purpose.** To implement guidelines and procedures consistent with federal and District law that protect the privacy of our consumers' health information. The governing privacy guidelines are described in this policy. Specific topics and procedures are addressed in the Department of Mental Health (DMH) Privacy Policies and Procedures Operations Manual (See Section 13 for distribution of this manual).

2. **Applicability.** DMH and its participating Network providers.

Network means an organized health care arrangement consisting of DMH, and every mental health provider that is certified, licensed, or otherwise regulated by DMH, or has entered into a contract or agreement with DMH for the provision of mental health services or mental health supports.

This policy replaces any requirements in existing Department policies that may contain different information relating to confidentiality of mental health information. Those policies shall be revised accordingly.

3. **Authority.** Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations at 45 Code of Federal Regulations Parts 160 and 164 ("HIPAA Privacy Rules"), and the District of Columbia Mental Health Information Act of 1978.

4. **Policy.**

4a. It is the policy of DMH to protect the privacy of consumers' health information that DMH and its participating Network providers create, receive or maintain in their respective roles as health care providers.

4b. Each workforce member with access to protected health information (PHI) must, at all times, comply with the policies and procedures set out in the DMH Privacy Policies and Procedures.

4c. Workforce members shall consult with their Privacy Officer or designee before they use or disclose PHI if there is any doubt regarding whether such use or disclosure is permitted by the DMH Privacy Policies and Procedures or by the HIPAA Privacy Rules.

4d. Failure to comply with the DMH privacy policies and procedures may subject DMH employees to discipline in accordance with Chapter 16 of the District Personnel Manual (DPM) and applicable collective bargaining agreements, and all workforce members to potential civil and criminal penalties (See Section 7 below).

4e. Only the DMH Privacy Officer, with approval from the DMH Director and other District approvals as required, may change the DMH Privacy Policies and Procedures.

5. **Privacy Officers, Agency Heads.**

5a. The DMH Privacy Officer is responsible for developing, maintaining, and implementing the DMH Privacy Policies and Procedures, and for overseeing full compliance with the DMH policies and procedures, the HIPAA Privacy Rules, the D.C. Mental Health Information Act and other

applicable federal and state privacy law.

5b. The DMH Privacy Officer shall serve as the Privacy Officer for DMH Authority level employees and as the senior Privacy Officer for the Department. Saint Elizabeths Hospital (SEH) and the DC Community Services Agency (DC CSA) shall have their own Privacy Officer who must also comply with the duties and responsibilities of the Privacy Officer as outlined in the DMH Privacy Policies and Procedures. Other Network providers shall designate personnel and establish systems to carry out the duties of a Privacy Officer as required by HIPAA.

Each Privacy Officer may delegate specific duties and responsibilities to designees who are trained to assist in carrying out the duties of the Privacy Officer. In addition, the Privacy Officers shall consult with their respective legal offices when situations arise that are beyond the scope of their knowledge.

5c. The DMH Director and each agency head shall ensure that the requirements of these policies and procedures are carried out, and that workforce members become familiar with and adhere to these policies and procedures.

5d. *After Regular Work Hours.* DMH Administrators-On-Call shall contact the Privacy Officer on call for their organization if questions regarding use and disclosure of PHI related to an emergency arise after regular working hours. Other Network participants shall also ensure that mechanisms are in place to appropriately address these issues after regular working hours.

6. Workforce Training.

6a. Each workforce member who may have access to or use of PHI shall receive training on the DMH Privacy Policies and Procedures as necessary and appropriate for the member to carry out his or her job functions.

6b. Training Process. The DMH Privacy Officer and Privacy Officers at the DC CSA and SEH shall work with the DMH Training Institute and their respective local training offices, and the DMH Division of Human Resources (DHR) to facilitate training DMH employees, including determining the appropriate training content needed by particular trainees and new hires to carry out their job functions. The DHR Director or designee shall coordinate training of newly hired members of our workforce as promptly as practical, but before the new hires are given access to or use of PHI. Other Network providers must ensure that their workforce members are appropriately trained.

6c. Training Timing.

- (1) Current Workforce. Existing workforce must complete privacy training.
- (2) New Hires. Newly hired members of our workforce must receive privacy training before they may have access to or use of PHI.
- (3) Retraining. Existing workforce members must receive retraining no later than 45 days after there is material change in their job functions or in our DMH Privacy Policies and Procedures that affects their access to or use of PHI.

6d. Training Documentation. Your Privacy Officer or training officer will document completion of training of each workforce member on our DMH Privacy Policies and Procedures, using a privacy training certificate. The DMH Privacy Officers or training officers will send a copy of the completed certificates to the DMH Division of Human Resources for inclusion in the personnel file of the DMH workforce member trained.

6e. *Assurance of Confidentiality.* Each DMH workforce member shall be provided and shall sign FORM 15, Assurance of Preservation of the Confidentiality and Security of Protected Health Information, after role-based training has been completed on these policies and procedures. This form shall be placed in the workforce member's personnel record. Other Network participants are encouraged to use this form or a similar process.

7. **Workforce Sanctions.** DMH workforce members who violate our DMH Privacy Policies and Procedures, the HIPAA Privacy Rules or the DC Mental Health Information Act (MHIA) or other applicable federal or state privacy law shall be subject to discipline in accordance with Chapter 16 of the DPM and applicable collective bargaining agreements.

In addition to the workplace sanctions, consumers can seek civil and criminal penalties for violation of the MHIA, and may file a complaint with the U.S. Department of Health and Human Services for violation of HIPAA.

8. **Reporting Workforce Privacy Violations.** Each member of our workforce is obligated to report promptly any suspected violation of our DMH Privacy Policies and Procedures, the HIPAA Privacy Rules, MHIA, or other applicable federal or state privacy law to their Privacy Officer or designee. Reports may be made anonymously. Each workforce member must cooperate fully with any investigation, corrective action or sanction instituted by their Privacy Officer.

9. **Mitigation.** Network participants shall initiate corrective action whenever an improper use or disclosure of PHI occurs by one of their workforce members or business associates.

10. **Retaliatory Acts.**

10a. Network participants shall not tolerate any workforce member who attempts to intimidate, threaten, coerce, discriminate or retaliate against an individual who:

- Exercises any right, including filing complaints, under the DMH Privacy Policies and Procedures or other privacy laws.
- Complains to, testifies for, assists or participates in an investigation, compliance review, proceeding or hearing by the Department of Health and Human Services (HHS) or other appropriate authority.
- Opposes any act or practice the individual believes in good faith is illegal under the Privacy Rule (provided the opposition is reasonable and does not involve illegal disclosure of PHI).

10b. A workforce member who suspects that another workforce member has violated the ban on retaliatory acts must report the suspicion to their Privacy Officer or designee. Reports may be made anonymously. Each workforce member must cooperate fully with any investigation, corrective action or sanction instituted by their Privacy Officer.

11. **Document and Record Retention.** The DMH, DC CSA, and SEH Privacy Officers, must ensure that all documentation required by our DMH Privacy Policies and Procedures and the HIPAA Privacy Rules are maintained at least six (6) years after the later of its creation or last effective date. Other Network providers must retain their documentation in compliance with HIPAA. Each Privacy Officer or designee will ensure the following information is maintained in written or electronic form:

- The DMH Privacy Policies and Procedures and each revision of them.
- The DMH Privacy Practices Notices, each revision of them, and all documentation relating to our distribution of them.

- Each authorization and authorization revocation.
- Each request from consumers for access, amendment, disclosure accounting, restriction, or confidential communication, and all other documentation relating to our compliance with our obligations with respect to consumers' rights.
- Each complaint and any material generated as a result of investigating and resolving the complaint.
- Documentation evidencing designation of each Privacy Officer and any delegation of duties and responsibilities to the Privacy Officer's designees, designation of personnel and record sets, and designations with respect to covered entity structures.
- Documentation relating to personal representative relationships, business associate relationships, group health plan and plan sponsor relationships, limited data sets, and de-identified health information.
- Documentation of workforce training and sanctions, mitigation plans, and other administrative requirements.
- Other documentation requested or required under our DMH Privacy Policies and Procedures or demonstrating our compliance with our obligations under the HIPAA Privacy Rules.

12. **Data Privacy Protection.** DMH and all Network providers shall implement and comply with reasonable and appropriate administrative, physical, and technical safeguards to secure the privacy of PHI against any intentional or unintentional use or disclosure in violation of the Privacy Policies and Procedures or the HIPAA Privacy Rules. (Also see Part VII for security policies and procedures).

13. **Distribution/Location of the Manual.** The DMH Privacy Policies and Procedures Operations Manual shall be disseminated throughout the Department and made available to Network providers. DMH and each Network provider shall ensure that a copy of the manual is provided to all of their programs that require its use. It shall be placed in a prominent location where it is accessible to all employees that use and/or disclose PHI.

Approved By:

Martha B. Knisley
Director, DMH

(Signature)

(Date)